УДК 28.23.15

ИДЕНТИФИКАЦИОННЫЙ ПОТЕНЦИАЛ РУКОПИСНЫХ ПАРОЛЕЙ В ПРОЦЕССЕ ИХ ВОСПРОИЗВЕДЕНИЯ*

Б. Н. Епифанцев[1], П. С. Ложников[2], А. Е. Сулавко[2], С. С. Жумажанова[1]

[1] *Сибирская государственная автомобильно-дорожная академия (СибАДИ), 644080, г. Омск, просп. Мира, 5*
[2] *Омский государственный технический университет, 644050, г. Омск, просп. Мира, 11*
E-mail: sulavich@mail.ru

Проведено сравнение возможностей естественного и искусственного интеллектов в задачах идентификации операторов информационно-вычислительной системы и их функционального состояния по особенностям воспроизведения рукописных паролей. Установлена причина значительного разброса вероятностей ошибок идентификации субъектов. Сделан вывод, что при современном уровне знаний лучший из достигнутых результат решения обозначенной задачи системой искусственного интеллекта приблизился к потенциально возможному. Обоснована целесообразность использования особенностей воспроизводимых рукописных паролей для распознавания функционального состояния операторов человеко-машинных систем в процессе профессиональной деятельности.

Ключевые слова: информационная безопасность, подсознательные движения, идентификация подписантов, искусственный интеллект, естественный интеллект, сравнение возможностей интеллектов, идентификация состояний субъекта.

DOI: 10.15372/AUT20160304

Введение. Неавторизованный доступ в информационно-вычислительные системы признан одной из самых опасных угроз для информационной безопасности [1]. Основной причиной инцидентов, связанных с нарушениями безопасности, являются действующие (31 %) и бывшие (27 %) сотрудники организаций, суммарный ущерб от деятельности которых составил за 2013 и 2014 годы более 42 млрд. долларов [2].

Существующая технология авторизации по предъявляемому паролю оказалась недостаточно эффективной. Это подтвердила дискуссия в Конгрессе США, по результатам которой установлено, что наиболее уязвимое место в системе безопасности — человеческий фактор. Пароль конкретного лица не является секретом для работающих с ним сотрудников [3].

В 2010 году на сайте Wikileaks были опубликованы сотни тысяч документов о военных операциях США в Ираке и Афганистане, в январе 2013 года Э. Сноуден раскрыл секретные данные Агентства национальной безопасности США. Ущерб от такого рода действий необычайно велик. Потребовалось заново проанализировать технологию допуска своих сотрудников к информационным ресурсам организации. Появилась необходимость введения дополнительного звена биометрической идентификации сотрудника при входе в систему в скрытом от него режиме [4]. Обеспечение скрытости этой операции исключает применение большинства эффективных систем на базе статических биометрических признаков.

*Работа выполнена при поддержке Министерства образования и науки РФ (задание № 212/2016).

Использование подсознательных движений оператора (динамических биометрических признаков) для решения идентификационных задач рассматриваемого назначения ограничено недостатком информации об их эффективности.

В последние годы интерес исследователей был сконцентрирован на распознавании субъектов по особенностям воспроизведения рукописных паролей, в качестве которых выступали автографы. Лучший результат по верификации таких паролей, продекларированный в конце 1990-х годов, составлял 4 % — сумма вероятностей ошибок 1-го и 2-го рода [5]. В 2000 году эта цифра возросла до 13 % [6], в 2002 снизилась до 2 % [7]. Лучший результат 2003 года — 2,78 % [8], 2008 — 3,3 % [9], 2012 — 1 % [10], 2013 — 2,8 % [11] и 1,2 % [12, 13]. Если расширить перечень результатов, полученных в этом направлении за обозначенный период времени, они будут различаться более значительно, чем приведённые, даже в случаях, когда применяемые алгоритмы идентификации были идентичны. Поэтому первоочередным следует считать решение вопроса о причинах столь существенного разброса публикуемых данных.

Обращают на себя внимание достигнутые значения вероятностей ошибок 1-го и 2-го рода. В [9] для идентификации подписантов использовались статические признаки подписи (размах, наклон почерка) и динамические (скорость и давление пера). Для оценки эффективности предложенного алгоритма проведены эксперименты, в которых 111 подписантов предприняли 2779 попыток входа в систему под своими рукописными паролями и 1100 попыток подделки паролей. Вероятности ошибок 1-го и 2-го рода оценены в 2,2 и 1,1 % соответственно. В [13] экспериментально получены вероятности ошибок 1-го и 2-го рода: 0,01 и 0,0033 при наличии в базе 150 эталонов, достоверность данных оценена в 0,99. Включение в алгоритм идентификации операций по реализации так называемых альтернативных сценариев авторизации и нахождению меры Хэмминга позволило снизить вероятность ошибки 2-го рода до 0,002. Возникает вопрос, можно ли считать, что приведёнными оценками идентификационный потенциал подсознательных движений при формировании рукописного пароля исчерпан и дальнейшие попытки получения более высоких показателей идентификации не имеют смысла?

В области защиты информации сформулирована новая задача: «создать защиту от того, кому разрешено всё в соответствии со служебными обязанностями» [4]. Предлагаемая технология её решения — «сценарий четырёх глаз», основанный на одновременной работе оператора и контролёра, принимается исполнителями без энтузиазма. Высказана точка зрения, что необходимо скрыто идентифицировать функциональное состояние оператора при входе в систему. Если принимается решение об отклонении его состояния от адекватного, об этом извещается служба безопасности. Содержится ли в формируемом на графическом планшете пароле информация о функциональном состоянии субъекта, которую можно было бы использовать для решения поставленной задачи?

Попытка получить ответы на перечисленные вопросы — цель данной работы.

Стабильность эталонов рукописных паролей идентифицируемых субъектов. Вероятности ошибок 1-го и 2-го рода определяются степенью пересечения эталонных описаний распознаваемых образов в пространстве признаков и отклонением этих описаний от реальных в момент проведения экспериментов по идентификации субъектов. В вышеотмеченных работах последний фактор влияния на результаты идентификации не обсуждался.

В то же время известно, что температура в помещении, предшествующая опыту, физическая нагрузка и ряд других причин (например, употребление никотина, алкоголя, лёгких наркотиков [14]) влияют на характеристики воспроизведения рукописного текста [15].

Для оценки степени воздействия внешних факторов на формирование рукописных паролей была привлечена группа студентов из 28 человек. Известно, что вероятность ошибки идентификации по биометрическим признакам зависит от количества классифицируемых

субъектов и используемых признаков [16]. В России распространены организации, в которых доступ к информационным ресурсам имеют 20–30 человек. Данное обстоятельство определило численность экспериментальной группы.

Каждый из привлечённых субъектов вводился в одно из четырёх функциональных состояний:

1) «адекватное состояние»: в течение беседы на отвлечённые темы частота пульса изменялась не более чем на 10 %;

2) «физическая нагрузка»: перед началом эксперимента испытуемый приседал 20 раз, частота пульса в 1,5–2,0 раза превышала аналогичный показатель в состоянии 1;

3) «отрицательные эмоции»: прежде чем генерировать автографы, испытуемый вдыхал нашатырный спирт, частота пульса заметно повышалась (в 1,25–1,5 раза);

4) «состояние покоя»: перед опытами испытуемый в изолированном помещении в течение 20 мин слушал успокаивающую музыку, частота пульса снижалась на 5–10 %.

Перечисленные состояния не включены в существующий классификатор функциональных состояний, рекомендованный в [17] и основанный на оценке параметров вариабельности сердечного ритма. Для ответа на вышепоставленный вопрос не обязательно использовать предложенный классификатор.

В каждом состоянии испытуемые на графическом планшете воспроизводили свой автограф 80 раз подряд. Рекомендуемая мощность обучающего множества образов находилась в пределах от $2m$ до $20m$ (m — число признаков) [18]. Данное условие определило количество воспроизводимых автографов. В компьютер вводились функции координат пера $x(t)$ и $y(t)$ и его давления на поверхность планшета $p(t)$. Параметры состояния сердечно-сосудистой системы, необходимые для принятия решения о переходе субъекта в новое состояние, регистрировались на холтеровском мониторе «Кардиотехника-04». Функции $x(t)$ и $y(t)$ преобразовывались в функции скорости перемещения пера $\upsilon_x(t), \upsilon_y(t)$.

Последующие операции по преобразованию процессов $\upsilon_x(t)$, $\upsilon_y(t)$, $p(t)$ и идентификации подписантов проводились в соответствии с алгоритмом, предложенным и обоснованным в [12]:

1. Разложение функций в ряд Фурье, использование 16 гармоник, нормирование амплитуд гармоник по энергии сигнала введённого пароля, нормализация колебаний длительности отдельных реализаций анализируемых сигналов. Необходимость выполнения последнего фрагмента операции обусловлена следующим обстоятельством. При разных скоростях воспроизведения пароля конкретным субъектом длительности регистрируемых процессов T будут отличаться, хотя их структура (семантическая составляющая автографа) сохраняется. Нейтрализовать влияние этого фактора на формирование эталона можно, оперируя не значениями частот k/T, а номерами гармоник $k = 1, 2, \ldots$. Введённое ограничение (16 гармоник) обусловлено результатами проведённых ранее исследований: $\sim$98 % энергии рассматриваемого вида сигналов переносится 16 гармониками.

2. Построение одномерных плотностей вероятностей нормированных амплитуд каждой гармоники (независимость признаков констатирована в [12]) и коэффициентов взаимной корреляции процессов $\upsilon_x(t)$, $\upsilon_y(t)$, $p(t)$, которые для всех состояний испытуемых принимались за эталонные. Графики плотностей вероятностей одного из признаков показаны на рис. 1 (при очередном эксперименте все перечисленные признаки ранжировались по информативности и часть из них, мало влияющих на результат, исключалась из рассмотрения).

3. Проведение вычислительного эксперимента по идентификации субъектов с помощью эталонов, полученных в адекватном состоянии, но когда испытуемый пребывает в одном из указанных выше состояний.

Найденные плотности распределения использовались для генерации значений признаков A_j. Было сформировано по 1000 значений A_j (метод статистических испытаний

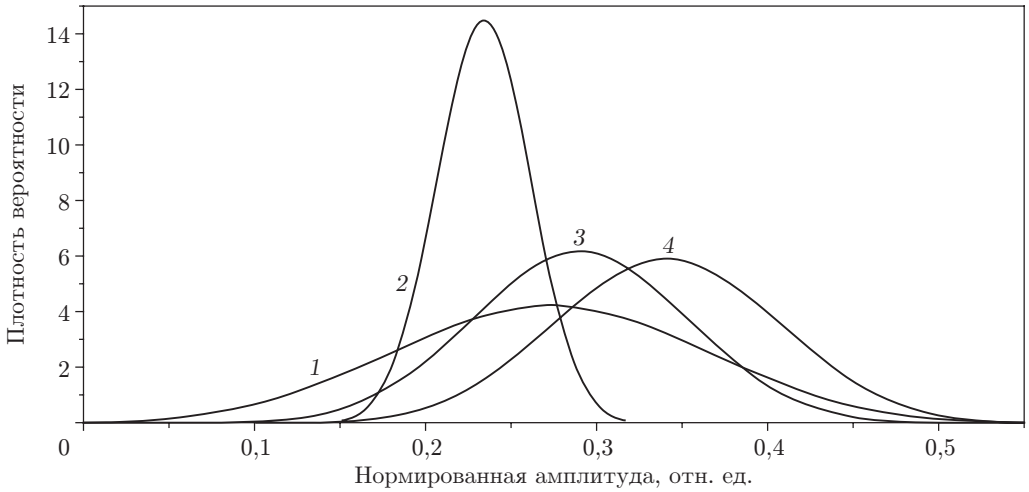

Рис. 1. Плотности вероятностей амплитуды первой гармоники процесса $p_{1i}(t)$ первого испытуемого в i-х состояниях: кривая *1* — адекватное состояние, *2* — физическая нагрузка, *3* — отрицательные эмоции, *4* — состояние покоя

Монте-Карло). Каждому из них соответствует вероятность гипотезы $P(A_j/H_i)$, которая определяется по сформированным в процессе обучения распределениям признаков. Последовательным применением формулы гипотез Байеса [19] вычислялись интегральные (финальные) вероятности гипотез:

$$P(H_i/A_j) = \frac{P(H_i/A_{j-1})P(A_j/H_i)}{\sum\limits_{i=1}^{n} P(H_i/A_{j-1})P(A_j/H_i)}.$$

На каждом шаге в качестве априорной вероятности использовалась апостериорная вероятность гипотезы, вычисленная на предыдущем шаге. На первом шаге все гипотезы считались равновероятными, т. е. $P(H_i/A_0) = n^{-1}$, где n — количество гипотез. При $j = N$ (N — количество признаков) по максимальному значению $P(H_i/A_N)$ принималось решение о принадлежности анализируемого рукописного пароля соответствующему субъекту. В данном эксперименте выбраны 40 признаков, ранжированных по минимуму пересечения плотности $P(A_j/H_i)$ с другими.

По результатам вычислительного эксперимента установлено:

— сумма вероятностей ошибок 1-го и 2-го рода идентификации субъектов по формируемым автографам в состоянии физической нагрузки при использовании эталонов, соответствующих адекватному состоянию, возрастала более чем в 3 раза;

— аналогичный показатель идентификации субъектов в состоянии отрицательных эмоций превышал полученный в адекватном состоянии более чем в 2 раза;

— регистрировалось увеличение вероятностей ошибочных решений, если субъекты находились в состоянии покоя.

Достоверность полученных оценок, определяемая количеством опытов и доверительным интервалом (0,02), составила 0,99.

Для подтверждения данных результатов проведён также натурный эксперимент по распознаванию субъектов в различных состояниях. В эксперименте использовалось 28 эталонов, полученных ранее по 80 реализациям. На этапе распознавания количество реализаций паролей субъектов в адекватном состоянии равнялось 497, в состоянии физической нагрузки — 510, в состоянии отрицательных эмоций — 37 и в состоянии покоя — 34.

Выбор значений первых двух цифр обусловлен стремлением достоверно оценить моменты распределения финальных вероятностей $P(H_i/A_N)$. При $N > 30$ значимых изменений моментов не фиксируется. В последующих экспериментах количество распознаваемых реализаций сокращено до 37 и 34. Для получения финальных вероятностей использовалась модифицированная формула Байеса [19]. Суммарные вероятности ошибок идентификации при переходе от адекватного состояния к другим увеличивались в среднем с 0,028 до 0,058. Достоверность этих результатов — 0,9 при доверительном интервале 0,015.

Полученные результаты свидетельствуют о существенном влиянии функционального состояния человека на надёжность его идентификации по особенностям воспроизведения автографов. Становится понятной причина значительного разброса приводимых в литературе данных о вероятностях ошибок распознавания субъектов по их рукописным паролям. Если эти данные не сопровождаются количественными показателями оценки функционального состояния субъектов, то они имеют ограниченную ценность.

Идентификационный потенциал воспроизводимого рукописного пароля в задачах распознавания субъектов. Достигнутый процент ошибочных решений при идентификации субъектов по динамике воспроизведения рукописных паролей на сегодняшний день составляет 1–2 %. Несмотря на значительные усилия, предпринимаемые для снижения этого процента, заметных успехов не наблюдается. Не достигнут ли предел возможностей искусственного интеллекта в решении задачи идентификации подписантов?

Одним из вариантов ответа на данный вопрос может быть сопоставление результатов идентификации человеком и системой искусственного интеллекта при решении однотипной задачи. Сложившаяся в прошлом веке точка зрения: «Ни одно техническое устройство не способно соперничать со зрительной системой человека. . .» [20] доминирует и в настоящее время.

При сравнении идентификационных возможностей естественного и искусственного интеллектов необходимо, чтобы количество предоставляемой информации для принятия решений было равным. Для обеспечения этого условия сформированные на графическом планшете функции $x(t)$, $y(t)$ и $p(t)$ пароля «Безопасность» записывались в базу данных и воспроизводились на экране монитора в темпе их написания. Давление пера $p(t)$ на планшет отображалось яркостью соответствующих фрагментов процесса.

При организации процесса обучения испытуемых учитывались особенности восприятия и запоминания предъявляемых образов человеком [21]. Субъект может сохранить в памяти и воспроизвести по завершении их показа 7 ± 2 единицы (правило Дж. Миллера). Неоднократное повторение предъявляемых образов позволяет увеличить это число в соответствии с законом К. Халла. Закон связывает вероятность правильного ответа с количеством представлений образов и имеет вид логистической кривой. Приводимые экспериментальные оценки такого числа для обеспечения указанной вероятности, близкой к единице, колеблются в диапазоне 20–30 предъявлений. Человеку свойственно забывать информацию. Данный процесс описывается законом Эббингауза: усвоенная информация за первые полчаса уменьшается на 3–5 %. Таким образом, если придерживаться положений стохастической модели обучения [21], для получения ответа на поставленный вопрос следует ограничиться в эксперименте пятью–семью образами, объёмом обучающей выборки для каждого испытуемого 20–30 единиц, проведением идентификации субъектов менее чем через полчаса после обучения.

На этапе обучения были привлечены десять субъектов, не знакомых с подписантами. Демонстрируемые им на экране процессы формирования рукописных паролей отмечались номером субъекта. Каждый из субъектов запоминал особенности воспроизводимых паролей по 30 предъявляемым реализациям идентифицируемых подписантов. Эти же реализации демонстрировались системой искусственного интеллекта для построения эталонов.

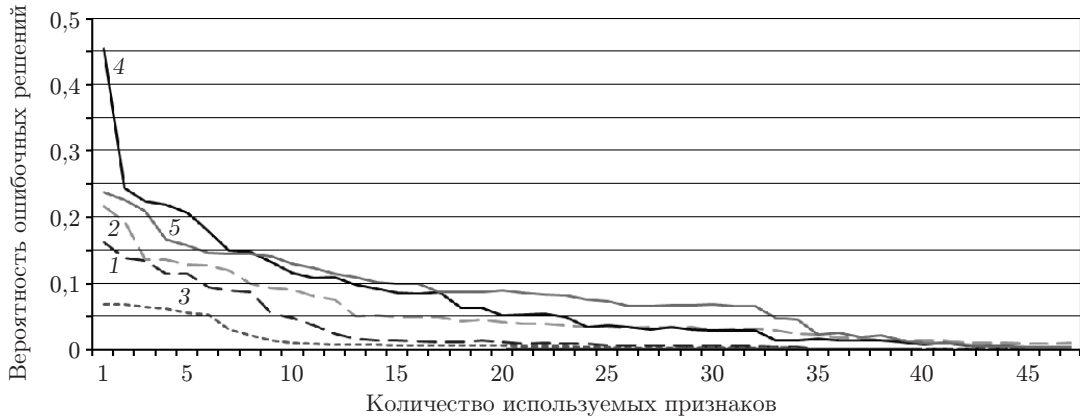

Рис. 2. Вероятности ошибочной идентификации адекватного состояния и состояния после употребления 100 мл шампанского пяти испытуемых в зависимости от количества используемых признаков рукописного пароля (кривые *1–5* — номера испытуемых)

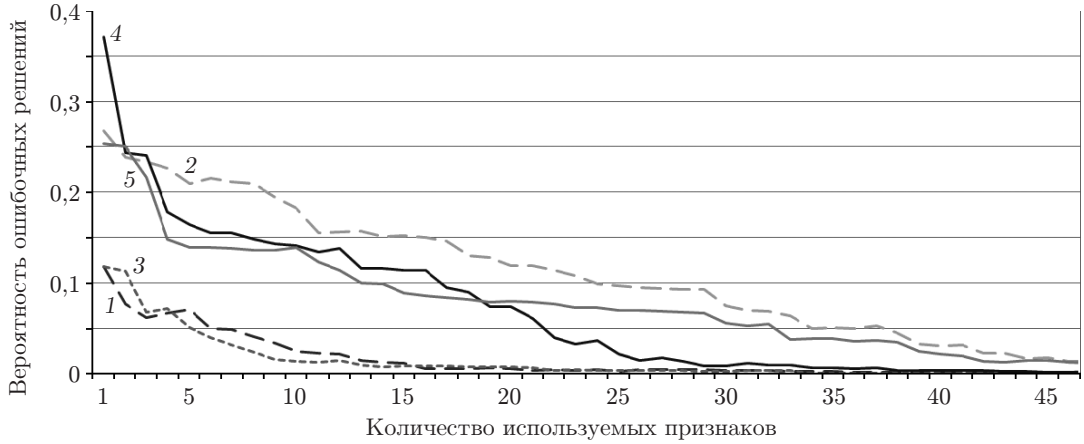

Рис. 3. Вероятности ошибочной идентификации адекватного состояния и состояния после воздействия нашатырным спиртом пяти испытуемых в зависимости от количества используемых признаков рукописного пароля (кривые *1–5* — номера испытуемых)

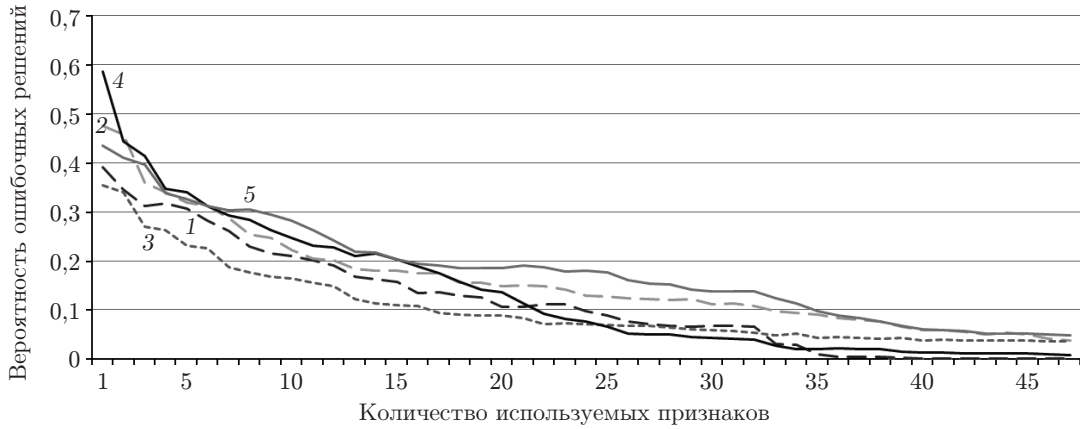

Рис. 4. Вероятности ошибочной идентификации адекватного состояния, после употребления алкоголя, после воздействия нашатырным спиртом пяти испытуемых в зависимости от количества используемых признаков рукописного пароля (кривые *1–5* — номера испытуемых)

На этапе распознавания «обученные» субъекты принимали решение о принадлежности воспроизводимого на мониторе рукописного пароля тому или иному подписанту. Все имеющиеся в базе данных пароли демонстрировались перед субъектами в случайном порядке. Эксперимент был разбит на пять этапов. На первом решалась задача верификации человека — его опознавание по воспроизводимому автографу сравнением с эталоном. На следующем этапе требовалось идентифицировать двух подписантов и т. д. Одновременно компьютерным зрением регистрировались принятые решения (алгоритм работы пояснён выше). Ошибочные решения отсутствовали. Для оценки малых вероятностей возможных ошибок необходимо располагать значительным объёмом статистического материала.

В результате экспериментов по оценке возможностей человека в задачах идентификации подписантов вероятности ошибочных решений составляли 0,11–0,348.

Зрительной системе не свойственны задачи идентификации образов в виде воспроизводимых кривых разных форм. Аналогичный вывод был сделан при сопоставлении возможностей человека и системы искусственного интеллекта в задачах распознавания изображений простых форм на фоне помех [20].

Полученные данные подтверждают предположение, что достигнутые показатели надёжности идентификации подписантов по особенностям воспроизведения ими паролей при современном уровне знания предмета исследования близки к предельно возможным.

О возможности идентификации функционального состояния субъекта по особенностям воспроизведения рукописного пароля. В последние годы к числу актуальных задач в области человеко-машинных систем отнесена задача разработки технологии распознавания эмоций оператора компьютера [22, 23]. Результаты её решения достаточно скромны: вероятность распознавания четырёх психоэмоциональных состояний колеблется от 62,7 [24] до 90 % [23]. Необходимо найти дополнительные признаки для достижения приведёнными вероятностями приемлемого уровня. Возможно ли рекомендовать в качестве таких признаков особенности воспроизведения рукописных паролей?

Для ответа на этот вопрос проведён следующий эксперимент. Формировались плотности распределения вероятностей первых 47 ранжированных по информативности признаков воспроизводимых рукописных паролей (обоснование признаков дано выше; исключены из рассмотрения последние четыре гармоники) каждого из пяти испытуемых в адекватном состоянии, по истечении 3 мин после употребления 100 мл шампанского и в состоянии отрицательных эмоций. Методом Монте-Карло генерировались по 1000 значений признаков. Описанным выше алгоритмом, основанным на формуле гипотез Байеса, идентифицировались состояния каждого из пяти испытуемых:

— адекватное и после употребления алкоголя;

— адекватное и отрицательные эмоции;

— адекватное — принятие алкоголя — отрицательные эмоции.

Полученные вероятности ошибочных решений в зависимости от количества применяемых признаков приведены на рис. 2–4.

По результатам вычислительного эксперимента вероятность правильной идентификации трёх состояний субъекта в использованном пространстве признаков превышает 0,94 и следует дать положительный ответ на поставленный вопрос.

Заключение. Достигнутый уровень надёжности идентификации подписантов компьютерным зрением по особенностям написания ими паролей (автографов) характеризуется суммарной вероятностью ошибок 1-го и 2-го рода в процентах. Аналогичные результаты для естественного интеллекта, полученные в подобных условиях эксперимента, существенно превышают эту вероятность. Следует признать, что при современном уровне знаний достигнутые результаты по распознаванию искусственным интеллектом подписантов, находящихся в одном и том же функциональном состоянии на этапах обучения и идентификации, близки к предельно возможным.

Учитывая, что обеспечить идентичность функциональных состояний субъекта в момент обучения системы искусственного интеллекта и на практике проблематично, целесообразно дальнейшие исследования в этом сегменте науки направить на создание технологии распознавания состояний. Использование семантической и эмоциональной составляющих рукописного пароля позволит повысить уровень защиты информации в системах организационного управления [25].

Одна из главных причин наблюдаемого разброса опубликованных результатов — неодинаковые функциональные состояния испытуемых в моменты формирования эталонов (обучения алгоритма) и проведения экспериментов по их идентификации.

СПИСОК ЛИТЕРАТУРЫ

1. **Information** Security Breaches Survey 2010. Technical report. URL: http://pwc.biogc.com/files/isbs-2010-report-final.pdf (дата обращения: 13.05.2014).
2. **Утечки** конфиденциальной информации. Отчёт Zecurion. 2014. URL: http://www.zecurion.ru/upload/iblock/fe3/Zecurion_Data_leaks_2015.pdf (дата обращения: 22.01.2015).
3. **Шнайдер Б.** Секреты и ложь. Безопасность данных в цифровом мире. С.-Пб.: Питер, 2003. 368 с.
4. **Эффект Сноудена.** Методы и технологии противодействия XVmatic // Специальная техника. 2013. № 5. С. 62–63.
5. **Xiao X. H., Leedham G.** Signature verification by neural networks with selective attention // Appl. Intell. 1999. **11**, Is. 2. P. 213–223.
6. **Wessels T., Omlin C. W.** A hybrid system for signature verification // Proc. of the IEEE-INNS-ENNS Intern. Joint Conf. Neural Networks. Como, Italy, 2000. Vol. 5. P. 509–514.
7. **Yoon H. S., Lee J. Y., Yang H. S.** An on-line signature verification system using hidden Markov model in polar space // Proc. of the 8th Intern. Workshop on Frontiers in Handwriting Recognition (IWFHR). Washington, USA: IEEE Computer Society, 2002. P. 329–333.
8. **Muramatsu D., Matsumoto T.** An HMM on-line signature verification algorithm // Proc. of the 4th Intern. Conf. AVBPA. Ser. Lecture Notes in Comput. Sci. Berlin — Heidelberg: Springer-Verlag, 2003. Vol. 2688. P. 233–241.
9. **McCabe A., Trevathan J., Read W.** Neural network-based handwritten signature verification // Journ. Comput. 2008. **3**, N 8. P. 9–22.
10. **Bashir M., Kempf F.** Advanced biometric pen system for recording and analyzing handwriting // Journ. Signal Process. Syst. 2012. **68**, N 1. P. 75–81.
11. **Boutellaa E., Bengherabi M., Harizi F.** Improving online signature verification by user-specific likelihood ratio score normalization // Proc. of the 8th Intern. Workshop on Systems, Signal Processing and their Applications (WoSSPA). IEEE, 2013. P. 296–300.
12. **Ложников П. С., Сулавко А. Е.** Технология идентификации пользователей компьютерных систем по динамике подсознательных движений // Автоматизация и современные технологии. 2015. № 5. С. 31–36.
13. **Епифанцев Б. Н., Ложников П. С., Сулавко А. Е.** Алгоритм идентификации гипотез в пространстве малоинформативных признаков на основе последовательного применения формулы Байеса // Межотраслевая информационная служба. 2013. № 2. С. 57–62.
14. **Maršálek T., Matoušek V., Mautner P. et al.** Coherence of EEG signals and biometric signals of handwriting under influence of nicotine, alcohol and light drugs // Neural Network World. 2006. **16**, N 1. P. 41–60.

15. **Hofer J., Gruber C., Sick B.** Biometric analysis of handwriting dynamics using a script generator model // Proc. of the "2006 IEEE Mountain Workshop on Adaptive and Learning Systems". IEEE, 2006. P. 36–41.
16. **Епифанцев Б. Н., Архипов А. А.** Об информативности признака асимметрии лица в задачах распознавания операторов эргатических систем // Автометрия. 2015. **51**, № 4. С. 31–39.
17. **Машин В. А.** К вопросу классификации функциональных состояний человека // Экспериментальная психология. 2011. **4**, № 1. С. 40–56.
18. **Ерош И. Л., Сергеев М. Б., Соловьев Н. В.** Обработка и распознавание изображений в системах превентивной безопасности. С.-Пб.: СПбГУАП, 2005. 154 с.
19. **Епифанцев Б. Н., Ложников П. С., Сулавко А. Е.** Сравнение алгоритмов комплексирования признаков в задачах распознавания образов // Вопросы защиты информации. 2012. № 1. С. 60–66.
20. **Красильников Н. Н.** Статистическая теория передачи изображений. М.: Связь, 1976. 184 с.
21. **Аткинсон Р., Бауэр Г., Кротерс Э.** Введение в математическую теорию обучения. М.: Мир, 1969. 486 с.
22. **Nogueira P. A., Rodrigues R., Oliveira E., Nacke L. E.** A hybrid approach at emotional state detection: Merging theoretical models of emotion with data-driven statistical classifiers // Proc. of the "2013 IEEE/WIC/ACM Intern. Joint Conf. on Web Intelligence and Intelligent Agent Technologies". IEEE, 2013. Vol. 2. P. 253–260.
23. **Cross C. B., Skipper J. A., Petkie D. T.** Thermal imaging to detect physiological indicators of stress in humans // Proc. SPIE. 2013. **8705**. 870501.
24. **Eom J.-S., Sohn J.-H.** Emotion recognition using facial thermal images // Journ. Ergonomics Society of Korea. 2012. **31**, Is. 3. P. 427–435.
25. **Белоконь С. А., Васильев В. В., Золотухин Ю. Н. и др.** Автоматизированные системы диспетчерского управления объектами повышенной опасности // Автометрия. 2011. **47**, № 3. С. 73–83.

Поступила в редакцию 10 марта 2015 г.